РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

дисциплина: Математические основы защиты информации и информационной безопасности

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Попова Юлия Дмитриевна

Группа: НФИмд-01-23

МОСКВА

2023 г.

Прагматика выполнения лабораторной работы

- Требуется реализовать шифр Цезаря с произвольным ключом k и Реализовать шифр Атбаш.

Цель работы

Приобретение практических навыков шифрования простой замены.

Выполнение лабораторной работы

1. Реализовали программу для шифра Цезаря (1/2)

```python
import sys

alpha = "а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я"
alpha = alpha.split()
password = list(input("Пароль: ").lower())
k = int(input("Сдвиг: "))
k = k % len(alpha)


uniq_letters = list()
for letter in alpha:
    if letter not in password:
        uniq_letters.append(letter)
if k == 0:
    cypher = password + uniq_letters
elif k <= len(alpha) - len(password):
    cypher = uniq_letters[-k:] + password + uniq_letters[:len(uniq_letters)-k]


print(alpha)
print(cypher)

while True:
    mess = str(input("Предложение, которое будет зашифровано с помощью шифра Цезаря (f - для завершения работы программы): "))
    if mess == 'f':
        break
```

1. Реализовали программу для шифра Цезаря (2/2)

```python
print(alpha)
print(cypher)

while True:
    mess = str(input("Предложение, которое будет зашифровано с помощью шифра Цезаря (f - для завершения работы программы): "))
    if mess == 'f':
        break

    cypher_mess = str()
    for symbol in mess:
        if symbol == ' ':
            cypher_mess += ' '
        else:
            cypher_mess += cypher[alpha.index(symbol)]

    print(cypher_mess)
```

2. Вывод работы первой программы

```
"C:\Users\Asuser\Desktop\магистратура\inf sec\lab1\venv\Scripts\python.exe" "C:\Users\Asuser\Desktop\магистратура\inf sec\lab1\main.py"
Пароль: пароль
Сдвиг: 3
['а', 'б', 'в', 'г', 'д', 'е', 'ё', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я']
['э', 'ю', 'я', 'п', 'а', 'р', 'о', 'л', 'ь', 'б', 'в', 'г', 'д', 'е', 'ё', 'ж', 'з', 'и', 'й', 'к', 'м', 'н', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы']
Предложение, которое будет зашифровано с помощью шифра Цезаря (f - для завершения работы программы): привет всем
зибярк яйре
Предложение, которое будет зашифровано с помощью шифра Цезаря (f - для завершения работы программы):
```

3. Реализовали программу для шифра Атбаш

```python
alpha = "а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я"
alpha = alpha.split()
alpha.append(' ')
cypher = alpha.copy()
cypher.reverse()


print(alpha)
print(cypher)

while True:
    finish = str(input("Предложение, которое будет зашифровано с помощью шифра Цезаря (f - для завершения работы программы): "))
    if finish == 'f':
        break

    cypher_mess = str()
    for symbol in finish:
        cypher_mess += cypher[alpha.index(symbol)]

    print(cypher_mess)
```

4. Вывод работы второй программы

```
"C:\Users\Asuser\Desktop\магистратура\inf sec\lab1\venv\Scripts\python.exe" "C:\Users\Asuser\Desktop\магистратура\inf sec\lab1\ata.py"
['а', 'б', 'в', 'г', 'д', 'е', 'ё', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я', ' ']
[' ', 'я', 'ю', 'э', 'ь', 'ы', 'ъ', 'щ', 'ш', 'ч', 'ц', 'х', 'ф', 'у', 'т', 'с', 'р', 'п', 'о', 'н', 'м', 'л', 'к', 'й', 'и', 'э', 'ж', 'ё', 'е', 'д', 'г', 'в', 'б', 'а']
Предложение, которое будет зашифровано с помощью шифра Цезаря (f - для завершения работы программы): привет всем
рпчюынаюоыу
Предложение, которое будет зашифровано с помощью шифра Цезаря (f - для завершения работы программы):
```

Вывод

В результате выполнения работы освоили на практике шифрование простой замены. Шифр Цезаря и Атбаш.